PT. KELLYS EXPRESS

SECURITY POLICY

Commercial & Confidential

KELLYS EXPRESS

Table of Contents

KELLYS EXPRESS

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at PT. Kellys Express, hereinafter, referred to as the **Practice**. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Practice with policies and guidelines concerning the acceptable use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Practice employees or temporary workers at all locations and by contractors working with the Practice as subcontractors.

Scope

This policy document defines common security requirements for all Practice personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Practice, entities in the private sector, in cases where Practice hasa legal, contractual or fiduciary duty to protect said resources while in Practicecustody. In the event of a conflict, the more restrictive measures apply. This policy covers the Practice network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Practice in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Practice domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Practice at its office locations or at remote locales.

Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

President Director – The person is responsible for the overall privacy and security practices of the company.

General Manager – The person is responsible for supervising the privacy, and security practices of the company.

Managers – The Confidentiality Officer is responsible for annual security training of allstaff on confidentiality issues.

CST – Confidentiality and Security Team

DoD – Department of Defense

Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP – File Transfer Protocol

HIPAA - Health Insurance Portability and Accountability Act

IT - Information Technology

LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.

NTFS – New Technology File Systems **–** NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

User - Any person authorized to access an information resource.

Privileged Users – system administrators and others specifically identified and authorized by Practice management.

Users with edit/update capabilities – individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**

Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changingrecords in a database. Their system access is limited to reading information only.

VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

VPN – Virtual Private Network – Provides a secure passage through the public Internet.

WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.

Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

Applicable Statutes / Regulations

The following is a list of the various agencies/organizations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

Privacy Officer

The Practice has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation,and maintenance of the Practice privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for the Practice is:

Name – Telephone Number[8]

Confidentiality / Security Team (CST)

The Practice has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Practice and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the President Director. The term of each member assigned is at the discretion of the President Director, but generally it is expectedthat the term will be one year. Members for each year will be assigned at the first meetingof the Quality Council in a new calendar year. This committee will consist of thepositions within the Practice most responsible for the overall security policy planning of the organization- the President Director, General Manager, and Managers, and as the current members of CST:

The CST will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identifyareas of concern within the Practice and act as the first line of defense in enhancing the security posture of the Practice.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The Managers or other assigned personnel is responsible for maintaining a logof security enhancements and features that have been implemented to further protect all sensitive information and assets held by the Practice. This log will also be reviewed during the quarterly meetings.

KELLYS EXPRESS

Employee Responsibilities

Employee Requirements

The first line of defense in data security is the individual Practice user. Practice users are responsible for the security of all data which may come to them in whatever format. The Practice is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear Identifying Badge so that it may be easily viewed by others -
In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in Practice facilities are provided with different colored identification badges[10]. Other people who may be within Practice facilities should be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel - It is the responsibility of all Practice personnel to take positive action to provide physical security. If you see anunrecognized person in a restricted Practice office location, you should challenge them as to their right to be there. All visitors to Practice offices must sign in at thefront desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Practice. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop with a Cable Lock - When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers.

Most Practice computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof, but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove. The use ofa cable lock helps to thwart this type of event.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Practice policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15)[11] minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Practice Corporate Assets - Only computer hardware and software owned by and installed by the Practice is permitted to be connected to or installed on Practice equipment. Only software that has been approved for corporate use by the Practice may be installed on Practice equipment. Personal computers supplied by the Practice are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Practice for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Practice employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

  Exception: Authorized information system support personnel, or others authorized by the Practice Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Practice has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" beforeapproval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Practice computers must be approved by the Practice.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Practice is strictly prohibited.

- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Practice is strictly prohibited.

Electronic Communication, E-mail, Internet Usage[12]

As a productivity enhancement tool, The Practice encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Practice owned equipment are considered the property of the Practice – not the property of individual users. Consequently, this policy applies to all Practice employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Practice provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Practice information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Practice information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Practice premises. The Practice encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Practice assets or resources.
    e) Harassment – The Practice strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Practice prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the Practice to monitor the content of any electronic communication, the Practice is responsible for servicing and protecting the Practice's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may bemonitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Practice reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Practice policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Internet Access

Internet access is provided for Practice users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Practice should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Practice routersand firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting Software Malfunctions

Users should inform the appropriate Practice personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Practice computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Managers as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The Managers should monitor the resolution of the malfunction or incident, and report to the CST Board the result of the action with recommendations on action steps to avert future similaroccurrences.

Report Security Incidents

It is the responsibility of each Practice employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person.A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Practice CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Practice CST must inform the other members as rapidly as possible. Each incidentwill be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibilityof the CST to provide training on any procedural changes that may be required as a resultof the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Practice Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Practice and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Practice policy and will result in personnel action, and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Practice computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Practice purchased software on home or on non-Practice computers or equipment.

Practice proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Practice without written consent of the respective supervisor or department head. It is crucial to the Practice to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Practice data to a non-Practice Computer System, the supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

The Practice Wide Area Network (“WAN”) is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Practice does not control non-Practice personal computers, the Practice cannot be sure of the methods that may or may not be in place to protect Practice sensitive information, hence the need for this restriction.

Internet Considerations

Special precautions are required to block Internet (public) access to Practice information resources not intended for public access, and to protect confidential Practice information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Practice Privacy Officer or appropriate personnel authorized by the Practice shall be obtained before:

- An Internet, or other external network connection, is established;
- Practice information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the Practice. The network can be used to market services related to the Practice, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Practice Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Installation of authentication and encryption certificates on the e-mail system
Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail
This software allows Practice personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Practice staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

De-identification / Re-identification of Personal Health Information (PHI)
As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged.

De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.
PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

KELLYS EXPRESS

Identification and Authentication

User Logon IDs

Individual users shall have unique logon ids and passwords. An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use/misuse of their individual logon id.

All user login ids are audited at least twice yearly[13] and all inactive logon ids are revoked. The Practice HR department notifies the ISO upon the departure of all employees and contractors, at which time login ids are revoked.

The logon id is locked/revoked after a maximum of three (3)[14] unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Practice systems or networks must have a completed and signed Network Access Form (Appendix A). This form must be signed by the supervisor or department head of each user requesting access.

Passwords

User Account Passwords

User ids and passwords are required in order to gain access to all Practice networks and workstations. All passwords are restricted by a corporate wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters[15].

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed every 90 days[16]. Compromised passwords shall be changed immediately.
Reuse - The previous twelve[17] passwords cannot be reused.
Restrictions on Sharing Passwords - Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.
Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

Confidentiality Agreement
Users of Practice information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix B). The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the PRACTICE information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Practice information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

Access Control
Information resources are protected by the use of access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Form. This form can only be initiated by the appropriate department head, and must be signed by the department head, and by the Privacy Officer or appropriate personnel.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, network, or EHR **only** upon the signature of the Privacy Officer or appropriate personnel who is

responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements
The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

Network Connectivity

Dial-In Connections
Access to Practice information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

Dial Out Connections
Practice provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place

Telecommunication Equipment
Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Privacy Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- Blackberry type devices
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

Permanent Connections
The security of Practice systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Practice systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

Emphasis on Security in Third Party Contracts
Access to Practice computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Practice Information Security Policy have been reviewed and considered.
- Policies and standards established in the Practice information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractualobligations.
- A detailed list of users that have access to Practice computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the datacollected under the agreement should be formally established before any users aregranted access.

- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls
Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a Practice router or firewall.

Malicious Code:

Antivirus Software Installation
Antivirus software is installed on all Practice personal computers and servers. Virus update patterns are updated daily on the Practice servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

> Configuration - The antivirus software currently implemented by the Practice is McAfee VirusScan Enterprise[18] . Updates are received directly from McAfee[19] which is scheduled daily at 5:00 PM[20].
> Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.
> Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Practice network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

New Software Distribution
Only software created by Practice application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Practice computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage Practice hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Practice computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Practice personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Practice computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not "bootable".

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Practice ownership at the time of employment. Nothing contained herein applies to software purchased by Practice employees at their own expense.

Encryption

Definition
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

Encryption Key
An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Practice shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. The Practice employs several methods of secure data transmission.

Installation of authentication and encryption certificates on the e-mail system
Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the Privacy Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail
This software allows Practice personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Practice staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

File Transfer Protocol (FTP)
Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

Secure Socket Layer (SSL) Web Interface
Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

Building Security

It is the policy of the Practice to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Practice strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Practice. All other facilities, if applicable, have similar security appropriate for that location.

- Entrance to the building during non-working hours is controlled by a security code system[21]. Attempted entrance without this code results in immediate notification to the police department.
- Only specific Practice employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The security code is changed on a periodic basis and eligible employees are notified by company e-mail or voice mail. Security codes are changed upon termination of employees that had access.
- The door to the reception area is locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s).
- The reception area is staffed at all times during the working hours of 8:00 AM to 5:00 PM[22].
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge(excluding patients), and be accompanied by a Practice staff member. In some situations, non-Practice personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times
- Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on each individual's job function or need to know[23] .
- The first floor of the building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department[24].
- All outside windows have glass breakage sensors which, if tripped, will result in immediate notification to the police department[25] .
- The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis[26].
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Practice considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Practice office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Practice network and/or hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Practice's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 90 days[27], is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

Required Equipment

Employees approved for telecommuting must understand that the Practice will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Practice Provided:

Practice supplied workstation[28] .
A cable lock to secure the workstation to a fixed object.
If using VPN, a Practice issued hardware firewall is required.

If printing, a Practice supplied printer.
If approved by your supervisor, a Practice supplied phone.

Employee Provided:

Broadband connection and fees,
Paper shredder,
Secure office environment isolated from visitors and family,
A lockable file cabinet or safe to secure documents when away from the home office.

Hardware Security Protections

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Practice personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.
VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing Practice information of any type. The Practice requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.
Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.
Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15[29] minutes of inactivity.

Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate Practice personnel for assistance. Protect external media by keeping it in your possession when traveling.
Transferring Data to the Practice**:** Transferring of data to the Practice requires the

use of an approved VPN connection to ensure the confidentiality and integrity of

the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Practice.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Practice Networks: Extreme care must be taken when connecting Practice equipment to a home or hotel network. Although the Practice actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Practice has no ability to monitor or control the security procedures on non-Practice networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Practice**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the Practice without the written approval of your supervisor.

Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Practice work environment, MUST have direct access to a shredder.
Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

Specific Protocols and Devices

Wireless Usage Standards and Policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Practice employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Practice laptops and mobile devices.

Approval Procedure - In order to be granted the ability to utilize the wireless network interface on your Practice laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Privacy Officer or appropriate personnel of the Practice. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by appropriate Practice personnel to setup your laptop and schedule training.
Software Requirements - The following is a list of minimum software requirements for any Practice laptop that is granted the privilege to use wireless access:

- Windows XP with Service Pack 3 (Firewall enabled)
- Antivirus software
- Full Disk Encryption
- Appropriate VPN Client, if applicable
- Internet Explorer 6.0 SP2 or Greater

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.
Training Requirements - Once you have gained approval for wireless access on your Practice computer, you will be required to attend a usage and security training session to be provided by the Privacy Officer or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Practice in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Practice networks. Every workstation or server that has been used by either Practice employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Practice data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Practice employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common practice within the Practice. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Practice networks. Transportable media received from an external source could potentially pose a threat to Practice networks. ***Sensitive data*** includes all human resource data, financial data, Practice proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Practice data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Practice.
- Non-Practice workstations and laptops may not have the same security protection standards required by the Practice, and accordingly virus patterns could potentially be transferred from the non-Practice device to the media and then back to the Practice workstation.

  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.
- Data may be exchanged between Practice workstations/networks and workstations used within the Practice. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:
  Data provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into Practice workstations or servers as long as the source of the media in on the Practice Approved Vendor list (Appendix D).
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Privacy Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the

employee or contractor or by the supervisor or department head immediately.

- When an employee leaves the Practice, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

The Practice utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Practice laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

KELLYS EXPRESS

Policy and Procedure

Retention / Destruction of Medical Information

Many state and federal laws regulate the retention and destruction of medical information. The Practice actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 6 years[300].

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST 800-88 guidelines.

Disposal of External Media / Hardware

Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of Excess Equipment

As the older Practice computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

Procedures

Notification:

The Information Systems or Technology Manager shall notify Practice management as soon as practicable in the event of:

- planned downtime of EHR systems,
- unexpected outage of EHR systems, and
- resumption of EHR services following an outage such that normal operations may resume.

Scheduling:

-
- If the EHR system is not operational or otherwise unavailable, the schedule printed theprevious day is retrieved. The center manager is tasked with maintaining a copy of thisschedule or assigning this duty as appropriate.
-
- If phones are operational, patient appointments may not be made. The operator shouldask for pertinent contact information and record a message using the paper telephone encounter form.

Patient Encounters:

Telephone encounters should be entered onto the paper telephone encounter form and transferred to a nurse for triage.

Out folders should be used as temporary charts.

Paper daybills should be used to record patient encounter for billing/tracking purposes. Check-in staff should verify patient's name, date of birth, telephone number, home address, and insurance information as available on the paper; schedule and record all changes on the daybill.

If the patient is a walk-in or new patient and demographic information is not available, paper registration forms should be filled out by check-in staff and placed in a temporary chart.

If co-pay information was available on the schedule, or if the patient has a co-pay amount listed on their insurance card, the check-in person should collect as appropriate.
Overhead pages through the telephone system will be used to notify nursing staff when a patient is ready to be taken back.
Paper progress note templates should be used to record usual nurse intake.
Out folder is placed on exam room door as before, using the flag system to notify provider that the patient is ready.
Provider records notes on paper progress notes.
Provider orders are recorded on paper progress notes, while recording the appropriate charges for orders on the paper daybill. The out folder is placed on the door and the flag system is used if nurse intervention is needed.
When the provider/nurse is finished with the patient, the provider will complete the encounter form (diagnosis, charges, and desired return appointment date/time) and have the patient go to check-out.
Encounter forms and progress notes should be kept for loading into the EHR for when the EHR operational and normal operations resume.

System Restoration:

Patient encounters occurring during system downtime should be entered into the system via the following procedures:

- The chief complaint should be appended with "- downtime progress note attached."

- Paper progress notes should be attached to electronic progress notes by scanning directly onto the progress note.

- Billing/insurance information should be updated as necessary as the diagnosis and charges from the encounter form are entered.
- Immunizations should be entered into the electronic progress notes.
- Scheduling telephone calls should be returned. A telephone encounter does not need to be entered into the EHR.
- Telephone encounters for all other issues should be entered into the system and routed as appropriate.

Additional Functions:

-
- The Practice manager is responsible for maintaining an adequate stock of paper forms inanticipation of system downtime.
- Faxes will be evaluated by a nurse for urgency of review by provider.
-
- Items requiring review by a provider will be placed in an out folder on the provider's
- desk.
-
- All other phone/fax information will be scanned into the patient's record when the EHRsystem is operational and normal operations have resumed.

KELLYS EXPRESS

Emergency Access “Break the Glass”

Policy Summary
The Practice has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The Practice has a formal, documented emergency access procedure enabling Practice workforce members to access the minimum EPHI necessary to effectively and efficiently treat patients in the event of a major medical emergency.

Purpose
This policy reflects Practice commitment to have emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency.

Definitions
Medical emergency means medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.
Electronic protected health information (EPHI) means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Electronic media means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Policy

1. The Practice has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The procedure includes:
    - Identifying and defining which the Practice workforce members authorized to access EPHI during an emergency.
    - Identifying and defining manual and automated methods to be used by authorized Practice workforce members to access EPHI during a medical emergency.
    - Identify and define appropriate logging and auditing that must occur when authorized Practice workforce members access EPHI during an emergency.
2. The Practice has a formal, documented emergency access procedure enabling Practice workforce members to access the minimum EPHI necessary to treat patients in the event of a medical emergency. Such access must be authorized by appropriate Practice management or designated personnel.
3. Regular training and awareness on the emergency access procedure is provided to all Practice workforce members.
4. All appropriate Practice workforce members have access to a current copy of the procedure and an appropriate number of current copies of the procedure should be kept off-site.

Scope/Applicability

This policy is applicable to all divisions and workforce members that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in definitions below.

HIPAA Security

Regulatory Category: Technical Safeguards
Regulatory Type: REQUIRED Implementation Specification for Access Control Standard
Regulatory Reference: 45 CFR 164.312(a)(2)(ii)
Rule Language:
"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (EPHI) during a medical emergency."

Scenario

"Break the Glass" refers to the practice of enabling a licensed practitioner to view a patient's medical record, or a portion thereof, under emergency circumstances, when that practitioner does not have the necessary system access privileges.

Policy Authority/Enforcement

The Practice Security Officer is responsible for monitoring and enforcement of this policy.

Procedures

Mechanism to Provide Emergency Access to EPHI

1. This process will bypass formal access procedures and is limited to medical emergencies.
2. The PD-G,-Managers may make requests foremergency access in writing.
3. The request should contain:
    a. The individual being granted the emergency access,
    b. Job title
    c. Reason for emergency access
    d. Date and time granted access
    e. The name of the individual granting access.
4. The Security Officer[31], or designated person, records information about emergency users and the emergency access rights assigned to them.
5. The system administrator and Security Officer[31] have created 2 administrator accounts solely for the purpose of emergency access. These accounts should be obviously named, such as breakglass01 and breakglass02 to allow for easy tracking of actions. These accounts and passwords are stored <these accounts need to be located where it would be obvious if they have been used or are missing, as though they were in a fire alarm box which required the glass to be broken to pull the alarm. A location such as in a sealed envelope taped to the side of a monitor in a very conspicuous place such as the nurses' station. Or, they can be locked in an area and require two employees, such as a manager and building security to access. There are a few EHR vendors who have "break glass" access available in their software, but that is not a common ability at this time.> [31]
6. The emergency access will be tracked and documented based on capabilities of the EHR. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate.
7. At the conclusion of the event that precipitated the granting of emergency access, the Security Officer ensures the breakglass accounts are disabled, and new ones created in anticipation of the next emergency.
8. Any inappropriate use of emergency access will be treated as a security incident, and may subject an employee to disciplinary action, up to and including termination.
9. Documentation concerning emergency access will be retained and maintained for at least six years from the date of creation.

Note:
When using a specific user account that provides full access to all EPHI (an administrator account) consider the following:

- Creating an extremely complicated password (but one an employee will be able to enter while under the stress of an emergency situation).
- Securing the password.
- Periodically changing the password.

Enforcement
Please refer to *IS-2.0 Sanction Policy* for details regarding disciplinary action against employees, contractors, or any individuals who violate this policy.

Sanction Policy

Policy
It is the policy of the Practice that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Practice will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.
The Practice will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Practice's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose
To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, Practice's security policies, Directives, and/or any other state or federal regulatory requirements.

Definitions
Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.
Sensitive information, includes, but not limited to, the following:

- Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.

- Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Practice.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Practice.
- Financial/accounting records – Any records related to the accounting practices or financial statements of the Practice.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.
Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations
Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense).

4	• Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions
In the event that a workforce member violates the Practice's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Practice shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions
Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Practice.

References
U.S. Department of Health and Human Services

Health Information Privacy. Retrieved April 24, 2009, from http://www.hhs.gov/ocr/privacy/index.html

Related Policies
Information Security Policy

Acknowledgment
I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for Practice Name[1].

Dated this_____day of_____, 20____.

_____
Signature of Employee/Contractor

e-Discovery Policy: Production and Disclosure

Policy
It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

Purpose
The purpose of this policy is to outline the steps in the production and disclosure process for health information and records related to e-discovery for pending litigation.

Scope
This policy addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures. Health information and records include both paper and electronic data related to relevant patient medical records and enterprise sources.

Procedure

Accurate Patient Identification

Responsible	Action
HIM	For litigation involving an individual's medical records, verify the patient's identity in the master patient index, including demographic information and identifiers including the medical record number. *[Note: When conducting searches, it is critical to accurately identify the correct patient and relevant information.]*
HIM	Note multiple medical record numbers, identifiers, aliases, etc., that will be used during the search process to find relevant information.

Subpoena Receipt and Response

Responsible	Action
Litigation Response Team	Upon receipt, subpoenas should be reviewed to determine that all elements are contained, the parties and the purpose are clearly identified, and the scope of information requested is clear. • Validate the served subpoenas before official acceptance. The validation process includes at a minimum: • Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and • Verification that the seal and clerk of the court signature are present and valid Review of the venue and jurisdiction of the court for the case and verification that the court is located within legal distance/mileage requirements.
HIM	Notify the Litigation Response Team that subpoena has been received and determine if a legal hold is in place. If not, the Litigation Response Team should determine whether a legal hold should be applied.
HIM	If the subpoena requests "any and all records," HIM and/or Legal Services should work with the judge and/or plaintiff's attorney to clarify the scope and type of information being requested. *[Note: The e-discovery process will identify vast volumes of data which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]*
Litigation Response Team/Legal Services	Provide direction to HIM in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Litigation Response Team/Legal Services	If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to PHI and will need to sign a Business Associate Agreement with this organization. Execute Business Associate Agreement as appropriate.

Search and Retrieve Process

Responsible	Action
Litigation Response Team	Identify the potential sources of information which may hold potentially relevant information, such as: ▪ Legal Health Record/EHR System (including source

	information systems such as nursing, ED, lab, radiology, etc.) ▪ Local area servers for the office ▪ Personal shares or personal folders on servers ▪ Dedicated servers for the organization ▪ Laptop and/or department computers ▪ Home computers, PDAs, SmartPhones ▪ E-mail, including archived e-mail and sent e-mail ▪ E-mail trash bin, desktop recycle bin ▪ Text/instant message archives ▪ Removable storage media (e.g., disks, tapes, CDs, DVDs, memory sticks and thumb drives) ▪ Department/office files such as financial records ▪ Personal desk files ▪ Files of administrative personnel in department/office ▪ Files located in department/office staff home ▪ Web site archives
HIM, Data Owners	Based on direction from the litigation response team on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (patient identifiers, search terms, key words, etc.) and conduct the search process. Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
IT	Provide assistance to HIM and Data Owners in the search and retrieval process for various systems and data sources.
HIM, Data Owners	Screen or filter the search results, eliminating inappropriate information (e.g., wrong patient, outside the timeframe, not relevant to the proceeding, etc.).
Legal Services	Review the content of the data/data sets found to determine relevancy to the proceeding and identify information that is considered privileged.
Legal Services, HIM, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

Production of Records/Data

Responsible	**Action**
HIM, Data Owners, IT	Determine the format the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data

	file, or review of material on-line. The format will vary depending on data, source, and agreement made in the Discovery Plan/Form 35.
HIM, Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, HIM, Data Owners, IT	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
Legal Services	Conduct final review of information before disclosing to requesting party.
Legal Services	Retain a duplicate of information disclosed to requesting party.

Charges for Copying and Disclosure

Responsible	**Action**
HIM, Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
HIM	Invoice requesting parties for allowable charges related to the reproduction of health information and records.
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

Testing and Sampling

Responsible	**Action**
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
HIM, Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Litigation	Assign a monitor for the outside party during their testing

Response Team, HIM	protocols.

Attorney/Third Party Request to Review Electronic Data

Responsible	Action
Litigation Response Team	Determine the procedures for allowing an attorney or third party to review the electronic records and search results on-line. This includes where the review will occur, system access controls, monitoring during the review session, and the charges, if any.
Legal Services, IT, HIM, Data Owners	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
HIM, Data Owners	Verify the outside party is allowed access to the record and systems by reviewing all supporting documentation (e.g., signed consent, credentials from retained firm, etc.).
HIM, Data Owners	Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by a patient or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.

Responding to Interrogatories, Deposition, Court Procedures

Responsible	Action
Legal Services	Legal Services manages the process for completion of the interrogatories and will coordinate processes related to depositions and testifying in court.
HIM (official record custodian)	HIM may provide information for an interrogatory, be deposed, or testify in court. HIM is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HIM also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system

	architecture, security practices, source applications, and the good faith operations from a technical infrastructure perspective.
Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The data owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the events the litigation. For example, a staff nurse who has made an entry into the medical record and is knowledgeable about the events of a case in litigation.
Business Associates/Third Parties	Business Associates/Third Parties may provide information for an interrogatory, be deposed, or testify in court. These include contractors and others who serve a variety of functions associated with a party's information but who themselves are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT Department.

APPROVALS:

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
[Specify Other Departments] [31]		Date:	

e-Discovery Policy: Retention

Policy
It is the policy of this organization to maintain and retain enterprise health information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

Purpose
The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic health information and records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes; and to ensure appropriate availability of inactive records.

Scope
This policy applies to all enterprise health information and records whether the information is paper based or electronic. It applies to any health record, regardless of whether it is maintained by the Health Information Management Department or by the clinical or ancillary department that created it.

Definitions

Data Owners: Each department or unit that maintains patient health records, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or her area are preserved, maintained, and retained in compliance with records management policies and retention schedules established by the Health Information Management Department *[or other designated authority]*.

Property Rights: All enterprise health information and records generated and received are the property of the organization. No employee, by virtue of his or her position, has any personal or property right to such records even though he or she may have developed or compiled them.

Workforce Responsibility: All employees and agents are responsible for ensuring that enterprise health information and records are created, used, maintained, preserved, and destroyed in accordance with this policy.

Unauthorized Destruction: The unauthorized destruction, removal, alteration, or use of health information and records is prohibited. Persons who destroy, remove, alter or use health information and records in an unauthorized manner will be disciplined in accordance with the organization's Sanction Policy.

Procedure

Responsible	**Action**
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
Record Committee	*[Note: This may be an existing committee, such as the Medical Record Committee, that has membership representing Legal, Compliance, IS/IT, Information Security, HIM, Clinical, and others as appropriate]* The record committee's role is to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.
HIM	HIM will convene the Record Committee as needed *[or at regular intervals]* and maintain responsibility for the following: • Review, maintain, publish, and distribute retention schedules and records management policies. • Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee. • Serve as point of contact for Records Coordinators. • Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance. • Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services. • Contract for destruction of paper and electronic records and certification thereof.

IT/HIM/Data Owners	IT/HIM/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following: • Transfer records to storage • Identify, control, and maintain records in storage • Retrieve and/or return records from/to storage • Document the destruction of records and the deletion of records from the records inventory • Monitor the records management process Record coordinators will obtain (if not already trained) and maintain records management skills.
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

	regular intervals] and maintain responsibility for the following: • Review, maintain, publish, and distribute retention schedules and records management policies. • Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee. • Serve as point of contact for Records Coordinators. • Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance. • Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services. • Contract for destruction of paper and electronic records and certification thereof.

IT/HIM/Data Owners	IT/HIM/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following: • Transfer records to storage • Identify, control, and maintain records in storage • Retrieve and/or return records from/to storage • Document the destruction of records and the deletion of records from the records inventory • Monitor the records management process Record coordinators will obtain (if not already trained) and maintain records management skills.
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.

Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.
E-mail Communication Retention	Depending on content, e-mail messages between clinicians and between patients and clinicians and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format. The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of *Messaging Policies* that establish disposal schedules for e-mail and manage their e-mail accordingly.
Development of Records Retention Schedules	Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. *[Note: minimum retention schedules are attached to this policy]*. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an

	application or database. Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators. Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section. Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department. Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—typically with e-mail, Microsoft “Office” applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to a “shared drive.” By saving a copy in this manner, IT will create an archive version of the saved document for a specified number of years after the user deletes the copy from the shared drive. Records with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or protected health information created or maintained on their workstations.

Storage and Destruction Guidelines

Active/Inactive Records	Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle. Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.
Storage of Inactive Records	All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.
Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include:

	[Note: specify based on local, state, and federal rule; these could potentially include recycling, shredding, burning, pulping, pulverizing, and magnetizing.] [31] A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal health information or other forms of confidential corporate, employee, member, or patient information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed. Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include: *[Note: specify based on local, state, and federal rules; these could potentially include: burning, shredding, or some other approach which renders the media unusable; degaussing, which uses electro-magnetic fields to erase data; or, preferred for magnetic media when media will not be physically destroyed, "zeroization" programs (a process of writing repeated sequences of ones and zeros over the information)]* [31]. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

APPROVALS:

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
[Specify Other Department]			

KELLYS EXPRESS

Breach Notification Procedures

Purpose
To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

Scope
This applies to all employees, volunteers, and other individuals working under contractual agreements with the Practice.

Definitions
State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Practice will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at_____-_____[32].
    a. Provide the Privacy Officer with as much detail as possible.
    b. Be responsive to requests for additional information from the Privacy Officer.
    c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
4. The Privacy Officer, in conjunction with the Practice's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized practice
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security practices
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the Practice's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
        i. The Privacy Breach Assessment tool will help aid the investigation.
    b. The Privacy Officer, in collaboration with the Practice's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – the Practice's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

1. The Privacy Officer will work with the department(s) involved, the Practice's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information

ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.

b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.

3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Practice's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the Practice will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the Practice if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Practice in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Practice's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the Practice will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.

   a. If necessary, this will include a security audit of physical, organizational, and technological measures.
   b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Practice's Sanction Policy.

Attachments
Appendix E: Privacy Breach Assessment

Related Policies
IS-2.0 Sanction Policy

KELLYS EXPRESS

Appendix A – Network Access Request Form

Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION

☐ New Employee ☐ New Contractor ☐ Existing User ☐ Temporary — Today's Date:

First Name: | Last Name: | *MI:

Position: | Department: / Supervisor:

☐ Full-time ☐ Part-time | Start date or Requested due date: / Temporary or Contractor end date, if known:

SECURITY & EMAIL

New Account:

☐ Network Account ☐ Email

☐ Security/Email similar to what existing user:

☐ Include in which E-mail Group(s): ☐ Remove from which E-mail Group(s):

☐ Include in which Security Group(s): ☐ Remove from which Security Group(s):

☐ Permit access to the following network location(s):

Drive Path Access: Read-only Read/write Full Access Remove Access Drive Path

Access: Read-only Read/write Full Access Remove Access Drive Path

Access: Read-only Read/write Full Access Remove Access

☐ Miscellaneous Needs *(Enter any other requests)*:

EHR ACCESS

☐ EHR Account

Roles & Access:

☐ Front Office Access: Read-only Read/write Full Access Remove AccessClinician

☐ Access: Read-only Read/write Full Access Remove Access Physician

☐ Access: Read-only Read/write Full Access Remove Access Accounting

☐ Access: Read-only Read/write Full Access Remove Access Records

☐ Management Access: Read-only Read/write Full Access Remove AccessReporting

☐ Access: Read-only Read/write Full Access Remove Access Administrator

☐ Access: Read-only Read/write Full Access Remove Access Other:

☐ Specify Access: Read-only Read/write Full Access Remove Access

☐ Miscellaneous Needs *(Enter any other requests)*:

HARDWARE & SOFTWARE

Hardware:

☐ Laptop ☐ Desktop ☐ Either Laptop or Desktop

☐ Screen protector ☐ Laptop bag ☐ Cable lock

☐ Multifunction printer ☐ Netgear Router ☐ Numeric keypad
☐ Standard inkjet printer ☐ Dual monitors ☐ Docking station
☐ iPhone ☐ iPad ☐ Windows Mobile Device

Software:
☐ Adobe Acrobat (full version) ☐ Email Encryption
☐ Microsoft Office Professional 2003 ☐ Microsoft Office Professional 2007
☐ MS Project 2007 ☐ MS Visio 2007 ☐ MS OneNote 2007
☐ Fax Server - *Specify level of access:*

☐ Miscellaneous Needs *(Enter any other requests)*:

TELEPHONY

Telephone:
☐ Desk Phone ☐ Softphone (IP Communicator)
☐ Desk phone currently exist at location. Current extension is:

Accessories:
☐ Wireless headset ☐ Wired headset

CELL PHONE / AIR CARD

☐ Cell phone ☐ Air Card

Accessories:
☐ Cell Phone Case/Holder ☐ Car Charger
☐ Miscellaneous Needs *(Enter any other requests)*:

BUILDING ACCESS

Access Requested for the following location(s):
☐ Medical Records Room ☐ Server Room
☐ Lobby ☐ Other, *Specify:*

Additional Access Restriction:
☐ After-Hours Access, *Specify Hours:*

Other Restrictions (be specific):

SPECIAL INSTRUCTIONS

Manager Checklist/Reminder:
- Signature below can be of the Department Head or the Data Owner if new network access is requested.
- Ensure employee badge is requested
- Schedule new employee orientation, if applicable
- Ensure name appears on any appropriate sign-in/out sheets
- Remember to have all new employees/contractors read and sign appropriate forms, i.e. Confidentiality Form (Appendix B)
- Request appropriate training/background:
    - HR Background Investigation
    - Security Training
    - Any additional training and/or background check

NAME	SIGNATURE	DATE
Department Head (Print Name)		
Privacy Officer / Appropriate Authority		

Appendix B – Confidentiality Form

RESPONSIBILITY OF CONFIDENTIALITY

I understand and agree to maintain and safeguard the confidentiality of privileged information of Practice Name[1]. Further, I understand that any unauthorized use or disclosure of information residing on the Practice information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

_____ _____

Date Signature

_____

Company/Firm

_____ _____

Date Signature of Practice Privacy Officer

Appendix C – Approved Software

The following list has been approved for use by the Practice. All software must be installed and maintained by the appropriate Practice personnel.

Software	Version	Approved by	Date	Description/Comments

KELLYS EXPRESS

Appendix D – Approved Vendors

Vendor	Primary Contact	Main Number	Product / Service	Description/Comments

KELLYS EXPRESS

Appendix E – Breach Assessment Tool

PRIVACY BREACH ASSESSMENT

1) Was Private Information Involved? ☐ Yes ☐ No

2) Was the Private Information encrypted? ☐ Yes ☐ No

3) Description of breach:

a) What data elements have been breached? Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.

b) What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

c) What was the date that the breach was discovered? _____

d) What is believed to be the date that the breach occurred? _____

2) Cause and Extent of the Breach

a) What is the cause of the breach?

b) Is there a risk of ongoing or further exposure of the information? ☐ Yes ☐ No

c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

d) Is the information encrypted or otherwise not readily accessible? ☐ Yes ☐ No

e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

a) How many individuals are affected by the breach?

1. Who was affected by the breach:

☐ Employees

☐ Customer-owners

☐ Volunteers

☐ Contractors

☐ Service providers

☐ Other individuals/organizations

4) Foreseeable Harm from the Breach

a) Is there any relationship between the unauthorized recipients and the data subject?
☐ Yes ☐ No

b) Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

KELLYS EXPRESS

1. What harm to the individuals will result from the breach? Harm that may occur includes:

☐ Security risk (e.g., physical safety)

☐ Identity theft or fraud

☐ Loss of business or employment opportunities

☐ Hurt, humiliation, damage to reputation or relationships

☐ Other (please specify):

d) What harm could result to the organization as a result of the breach?

☐ Loss of trust in the organization

☐ Loss of assets

☐ Financial exposure

☐ Other (please specify):

e) What harm could result to the public as a result of the breach?

☐ Risk to public health

☐ Risk to public safety

☐ Other (please specify):

1. Privacy Act Analysis
    a. Determine whether the breached information was in the control and possession of a Federal agency. If not, the Privacy Act does not apply and the analysis below is not necessary.
    b. Determine if the incident poses a risk to individuals. The following factors shall be considered when assessing the likely risk of harm and level of impact for a potential or confirmed privacy breach:
        i. Nature of the data elements breached in light of their context and the broad range of potential harms that may result from their disclosure to unauthorized individuals;
        ii. Potential harm to reputation of individuals;
        iii. Potential for harassment or prejudice;
        iv. Potential for identity theft, including any evidence that breached information is actually being used;
        v. Number of individuals affected;
        vi. Likelihood that breach was the result of a criminal act or will result in criminal activity;
        vii. Likelihood the information is accessible and usable by unauthorized individuals;
        viii. Likelihood the breach may lead to harm; and
        ix. Ability to mitigate the risk of harm.
    c. If an identity theft risk is present, tailor the response to the nature and scope of the risk presented. Notice may not be required in all circumstances, so the response team should assess the situation and determine if notification to individuals is necessary. In some cases, notification may actually increase a risk of harm, in which case <Practice> should delay notification until proper safeguards can be instituted. The analysis of whether notification is necessary should be based on the following factors:
        i. Number of individuals affected;
        ii. Urgency with which individuals need to receive notice;
        iii. Whether other public and private sector agencies need notification, particularly those that may be affected or may play a role in mitigating the breach;
        iv. Contact information available for affected individuals (first-class mail shall be the primary means for providing notification, but telephone or email may be appropriate when there is an urgent need); and
        v. Whether media outlets may be the best way to alert affected individuals and mitigate any risk.
    d. Written notification should include the following elements:

i. Brief description of what happened, including the date of the breach and its discovery;
ii. Description of the types of information involved in the breach;
iii. Statement whether the information was protected, if such information would be beneficial and would not compromise security;
iv. Steps individuals should take to protect themselves from harm;
v. What <Practice> is doing to investigate and mitigate the breach; and
vi. Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address and postal address.

e. If the <Practice> response team determines that public notification through the media is necessary, it should also post notification of the breach on its website, with the same information required for written notification to the individual. The posting should provide answers to frequently asked questions and other talking points.

2. State Data Breach Analysis
   a. Identify the state of residence of all individuals affected by the breach.
   b. Consult individual state data breach statues to determine if a state's particular data breach statute is applicable to <Practice>.
   c. Consult individual state data breach statutes to determine if a breach has occurred under a state's particular data breach statute.
   d. Consult individual state data breach statutes to determine breach notification steps to take in accordance with a state's particular data breach statute.
3. HIPAA/HITECH Analysis
   a. Determine whether the breached information was Protected Health Information (individually identifiable health information as defined by HIPAA). If not, HIPAA/HITECH breach reporting requirements do not apply and the analysis below is not necessary.
   b. If breached information was PHI, determine whether the PHI was secured or unsecured. Unsecured PHI is defined as PHI that is not secured through a means that HHS has approved as rendering the PHI unusable or unreadable to unauthorized persons.[1] If PHI was secured, no reporting is necessary under HIPAA and you can proceed to Step 2.

[1] As of the date of drafting, the following guidance was provided – COVERED ENTITY should review published guidance periodically to see if additional guidance was issued:
1) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and are judged by HHS to meet this standard.

c. If PHI was unsecured, it constitutes an official breach under HIPAA if it "compromises the security or privacy of the PHI" and does not meet one of the exceptions to breach.
    i. Compromises the security or privacy – this means that it poses a significant risk of financial, reputational or other harm to the individual. Sections 2 and 4 of the Privacy Breach Questionnaire should assist with this analysis. Key factors to consider:
        1. To whom was the information disclosed?
        2. What type of information was breached?
        3. How easily can the information be redistributed?
    ii. Exceptions to breach (these factors are fairly subjective and any analysis resulting in the conclusion that a disclosure meets one of these exceptions should be documented and retained for seven years):
        1. Good faith and unintentional acquisition, access or use by a person working under the authority of a covered entity or business associate, which is within the scope of authority and does not result in further use or disclosure.
        2. Disclosures between persons at the same covered entity, business associate or organized health care arrangement if persons are authorized and information will not be further used or disclosed.
        3. Disclosure where the covered entity or business associate has the good faith belief that the information could not have been retained (for example, a person drops their jump drive overboard on a moving cruise ship).

d. If the disclosure is found to meet one of these exceptions, or is not found to compromise the security or privacy of the PHI, proceed to Step 2. If the disclosure does not meet one of the exceptions to breach, and it is found to compromise the security or privacy of the PHI, the next step is to

---

i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

ii) Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140- 2. These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated.

2) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

determine how to mitigate the breach and protect the individual. Part of the mitigation and protection efforts would include notification, but they may also include instituting additional security measures, changing a person's account number, notifying police of the breach and other appropriate measures.

e. After determining and instituting mitigation and protection efforts, <Practice> must fulfill its obligations to notify the affected individuals of the breach. Notice must be provided within 60 days of discovery[2], unless authorized to delay by law enforcement personnel. First, <Practice> should determine how notice should be sent to the individual. The following rules apply:
    i. If contact information is sufficient and no more than 500 residents in the state are affected, written notification should be sent by first class mail.
    ii. If contact information is not sufficient for more than 10 individuals, notification must also be on the <Practice> home page and in major media (print or broadcast).
    iii. If more than 500 residents are affected, notification must also be made to major media, even if contact information is sufficient for all affected persons.
f. Notice should be carefully drafted to include the following required information, without any unnecessary information that may result in additional questions or concerns from affected individuals:
    i. Brief description of the breach, including the date of the breach and date of discovery.
    ii. Description of the types of PHI involved.
    iii. Steps the individual should take to protect themselves.
    iv. Brief description of steps <Practice> is taking to mitigate, investigate and protect (careful not to disclose information that could hamper any ongoing investigation).
    v. Contact procedures for questions or additional information, including a toll-free telephone number, email, Web site or address.
g. If more than 500 persons are affected, notice must also be provided to the U.S. Department of Health and Human Services. If 500 or less are affected, the notice should be kept in an annual log of breaches.

1. <u>Breach Analysis Follow-Up:</u> Once the breach analysis is complete and notice is provided, <Practice> should review policies, procedures and security measures to incorporate any necessary updates or changes.

[2] Discovery is defined as when the breach is known or should reasonably have been known.